The Feasibility of Quantitative Assessment of Security

Catherine Meadows
Center for High Assurance Computer Systems Naval Research Laboratory
Washington, DC 20375

In general, quantitative models of security have not met with a very warm acceptance. This has been a result of a number of factors. First of all, research in security has largely concentrated on high-assurance systems for which quantitative measures may not be realistic. Secondly, research in security has focussed on confidentiality, which is, at least in theory, possible to guarantee to a high degree of assurance even when most of the system is assumed to be actively trying to subvert the security policy. Thirdly, research in security generally operated in isolation from consideration of other system requirements.

However, all this has been changing. More interest in security is being shown by the commercial sector, which is more interested in cost-effort tradeoffs that achieving the highest degree of security possible. Also, more interest is being shown in systems that have other critical requirements besides security, such as real-time requirements or fault-tolerance. These requirements may come into conflict with security requirements, and some means are needed to quantify the tradeoffs between the competing properties.

As a result there has been a growing body of work on quantititative assessment of different security properties. The work of Kailar, Stubblebine and Gligor develops metrics for the the security of certain kinds of cryptographic protocols [KG94]. Other recent work has focussed on measuring the capacities of covert channels so they can be traded off against the real-time requirements of a system [Gra93, MM92]. Still other work, such as Gong's [Gon93], trades off various security goals of key distribution protocols against such performance metrics as number of messages and number of rounds of communication.

Although this kind of work is a promising start to developing a quantitative assessment of security, in general recent work has concentrated on quantitative measures of isolated security properties. What is lacking is some means of integrating these various approaches. By integration I mean, not only the integration of metrics for different security properties, but integration of the results of applying a single metric to different parts of a system. For example, a great deal of work has been done on measuring the capacity of isolated covert channels. But although there has been some work on measuring the capacity of composed or parallel channels [TG88, Tro90, Wit90], in general the problem of measuring the "leak rate" of an entire system has not received very widespread attention.

Given the lack of theoretical underpinnings at the most basic level, it is not surprising that more ambitious attempts to measure the likelyhood that the security of a computer system can be breached are not very convincing. What we need if more work from the ground up. We need to study closely the results of applying a a few metrics to the same component, and the result of applying a single metric to different components to the same system. Once we understand the results of integrating metrics on this small scale, we will be much better able to understand the feasibility of integrating them over an entire system.

References

[Gon93] L. Gong. Lower Bounds on Messages and Rounds for Network Authentication Protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pages 26–37. ACM Press, November 1993.

[Gra93] J. W. Gray III. On Introducing Noise into the Bus Contention Channel. In *Proceedings of the 1993 IEEE Symposium on Security and Privacy*, pages 90–98. IEEE Computer Society Press, May 1993.

[KG94] R. Kailar and V. Gligor. On the Security Effectiveness of Cryptographic Protocols. In *Proceedings of DCCA4*. 1994.

[MM92] I. S. Moskowitz and A. R. Miller. The Influence of Delay Upon an Idealized Channel's Bandwidth. In *Proceedings of the 1992 IEEE Symposium on Security and Privacy*, pages 62–67. IEEE Computer Society Press, May 1992.

[TG88] C.-R. Tsai and V. D. Gligor. A Bandwidth Computation Model for Covert Storage Channels and its Applications. In *Proceedings of the 1988 IEEE Symposium on Security and Privacy*, pages 108–121. IEEE Computer Society Press, May 1988.

[Tro90] J. Trostle. The Serial Product of Controlled Signalling Systems: A Preliminary Report. presented at Computer Security Foundations Workshop III, June 1990.

[Wit90] T. Wittbold. Networks of Covert Channels. presented at Computer Security Foundations Workshop III, June 1990.